10/586952
IAP11 Rec'd PCT/PTO 25 JUL 2006
PCT/CN2005/000159

Method for Upgrading the Communication Device

Field of the Technology

The present invention relates to communication field, more particularly to a method for updating communication equipment.

Background of the Invention

In the communication field, as new technologies and new services continuously emerge, the software of the communication equipment needs to be updated frequently, so as to maintain and optimize the communication network and provide more extensive and better communication services. Software update involves almost all communication equipment, such as exchangers, routers, Integrated Access Devices (IADs) and so on.

In all the existing software update procedures, the software to be updated is stored in an independent server, and then a data transmission connection is established between this server and the communication equipment to be updated, so that the software stored in the server can be transmitted to the communication equipment. During the update procedure, the corresponding files of the software stored in the server are directly transmitted to the communication equipment, and then the communication equipment loads the software to replace the old files with the new files, and the equipment is updated accordingly.

However, in the existing methods for updating equipment, the communication equipment does not back up the old configuration data which includes the user data, therefore during the software update procedure, if the communication equipment is powered off or the updated files error happens and so on, the old configuration data may be lost, which can bring great loss to the operators. In other words, the risk of losing data during the equipment update procedure exists in the prior art, which affects the security of the equipment update.

In addition, in the existing methods for updating equipment, the software update procedure is not monitored. If an error occurs during the update procedure, e.g., the communication equipment is powered off or the updated files error happens, the old service ability of equipment may not be inherited after the update procedure is finished, which may lead to unsuccessful equipment update and harm the security of the equipment

update.

Moreover, in the existing communication equipment, the old software version is usually not saved during the update procedure, so the old software version is not available to the equipment anymore in the case of unsuccessful update. Therefore, after the unsuccessful update, the communication equipment may change into failure or fault and cannot function normally, which greatly affects the security of the equipment update.

Summary of the Invention

In view of the above, the present invention is to provide a method for updating equipment that can implement a secure update, so as to avoid data loss from happening during the update procedure and make sure that the update is successful.

The present invention discloses a method for updating communication equipment in a communication system through a server, which stores updated files used for updating the communication equipment. The method at least includes:

backing up configuration data in the communication equipment to the server;

downloading the updated files to the communication equipment from the server, and loading the updated files to the communication equipment to implement the communication equipment update;

recovering the configuration data backed up in the server to the communication equipment.

Preferably, the step of backing up the configuration data in the communication equipment to the server further includes: the server monitoring the backup procedure of the configuration data and judging whether the configuration data are successfully backed up, if yes, executing the step of downloading the updated files to the communication equipment from the server and loading the updated files to the communication equipment to implement the communication update; otherwise, instructing the communication equipment to execute the backup operation for the configuration data again.

Hereby, the step of the server judging whether the configuration data are successfully backed up includes: judging whether a backup failure message is received from the communication equipment or judging whether the backup operation exceeds a scheduled

time. Moreover, before instructing the communication equipment to execute the backup operation for the configuration data again, the method further includes: notifying a user that the current configuration data backup has failed and asking the user whether to back up the data over again; after receiving the user's instruction to back up the data over again, executing the step of instructing the communication equipment to execute the backup operation again; otherwise, ending the current process.

When the communication equipment is an Integrated Access Device (IAD), and the server is a File Transfer Protocol/Trivial File Transfer Protocol (FTP/TFTP) server, the step of backing up the configuration data in the communication equipment to the server further includes:

an IAD Management System (IADMS) sending a Simple Network Management Protocol (SNMP) backup configuration data command to the IAD;

and the step of backing up the configuration data in the communication equipment to the server includes:

after receiving the SNMP backup configuration data command, the IAD transmitting the configuration data files to the specified FTP/TFTP server via the FTP/TFTP protocol.

The configuration data include one or more than one type among user data, port data, protocol parameter data and default parameter data for guaranteeing the normal operation of the equipment.

Preferably, the step of downloading the updated files to the communication equipment from the server and loading the updated files to the communication equipment to implement the communication update further includes: the server monitoring the update procedure of the communication equipment and judging whether the update is successful, if yes, executing the step of recovering the configuration data backed up in the server to the communication equipment; otherwise, instructing the communication equipment to execute the update operation over again.

Hereby, the server judging whether the update is successful includes: judging whether an update failure message is received from the communication equipment or judging whether the update operation exceeds the scheduled time. Moreover, before instructing the communication equipment to execute the update operation again, the method further

includes: notifying the user that the current update has failed and asking the user whether to update the equipment over again or not; after receiving the user's instruction to update the equipment over again, executing the step of instructing the communication equipment to execute the update operation again; otherwise, ending the current process.

The method may further include a step of storing an old software version in the communication equipment before executing the update operation, and a step of instructing the communication equipment to recover the current software to the old version before instructing the communication equipment to execute the update operation over again.

When the communication equipment is the IAD, and the server is the FTP/TFTP server, the step of downloading the updated files to the communication equipment from the server and loading the updated files to the communication equipment to implement the communication update further includes:

the IADMS sending an SNMP update command which includes the address information of the FTP/TFTP server and the name information of the updated files;

and the step of downloading the updated files to the communication equipment from the server and loading the updated files to the communication equipment includes:

after receiving the SNMP update command, the IAD downloading the updated files corresponding to the updated files name from the specified FTP/TFTP server via the FTP/TFTP protocol, and then loading the updated files.

Preferably, the step of recovering the configuration data backed up in the server to the communication equipment further includes: the server monitoring the recovery procedure of the configuration data, and judging whether the configuration data are successfully recovered, if yes, ending the current process; otherwise, instructing the communication equipment to execute the recovery operation for the configuration data over again.

Hereby, the server judging whether the configuration data are successfully recovered includes: judging whether a recovery failure message is received from the communication equipment or judging whether the recovery operation exceeds the scheduled time. Moreover, before instructing the communication equipment to execute the recovery operation for the configuration data over again, the method further includes: notifying the user that the current configuration data recovery has failed and asking the user whether to

recover the configuration data over again; after receiving the user's instruction to recover the configuration data over again, executing the step of instructing the communication equipment to execute the recovery operation over again; otherwise, ending the current process.

When the communication equipment is the IAD, and the server is the FTP/TFTP server, the step of recovering the configuration data backed up in the server to the communication equipment further includes:

the IADMS sending an SNMP recovery configuration data command which includes the address information of the FTP/TFTP server and the name information of the configuration data files;

and the step of recovering the configuration data backed up in the server to the communication equipment includes:

after receiving the SNMP recovery configuration data command, the IAD downloading the configuration data files corresponding to the configuration data files name from the specified FTP/TFTP server via the FTP/TFTP protocol, and then loading the configuration data files.

The step of recovering the configuration data backed up in the server to the communication equipment further includes a step of modifying the format of the configuration data.

It can be seen from the above-mentioned technical schemes that, besides the equipment update by directly downloading the updated files and loading the updated files according to the prior art, the present invention further includes the process of backing up the configuration data before the update and recovering the configuration data after the update, so that data loss will not happen when the communication equipment power off happens or the update is unsuccessful and the old software version needs be maintained. So the present invention can avoid great loss for the operators due to the data loss and the security of the equipment update is improved accordingly.

During the procedures of backing up the configuration data, updating the software and recovering the configuration data, the communication equipment operation is monitored all the time to judge whether the operation is successful. If the operation is unsuccessful,

the corresponding operation will be executed again automatically, so that the configuration data can be backed up, the software can be updated and the configuration data can be recovered again even if the communication equipment is powered off or the update is unsuccessful. Therefore, the present invention can guarantee the update is successful anyway and thus improve the security of the equipment update.

Moreover, in the present invention, the old software version can be stored before the update, so that the old software version is available once the update is unsuccessful. In the prior art, once the update is unsuccessful, new software cannot be run and the old software is not available, so the communication equipment changes into failure or fault, while the present invention can prevent such situation from happening and thus further improve the security of the equipment update.

Brief Description of the Drawings

Figure 1 is a flowchart illustrating the equipment update method according to one embodiment of the present invention.

Detailed Description of the Invention

The present invention will be further described in detail hereinafter with reference to the accompanying drawings and specific embodiments.

The communication equipment can be the equipment utilized in any fixed or mobile communication networks, such as exchangers, routers, Integrated Access Devices (IADs) and so on. Hereby the IAD can be the video telephone, the Media Gateway Control Protocol (MGCP) IAD, the Internet Protocol (IP) telephone terminal or others. The following embodiment will be illustrated taking the IAD for example, but those skilled in the art should understand that all the above illustrations can be applied in the other communication equipment without any obstacles.

In the prior art, the data can be easily lost and the software update is not guaranteed to be successful. In order to solve such problems, processes of backing up the configuration data, recovering the configuration data and monitoring the whole software update procedure are added to the present invention. Figure 1 is a flowchart illustrating the whole equipment update method after adding the above-mentioned processes.

As shown in figure 1, in step 100, the configuration data are backed up at first. Specifically, firstly the FTP/TFTP server information is configured to the IAD through the IADMS, and then the IADMS sends an SNMP backup configuration data command to IAD. After receiving this command, the IAD transmits the configuration data to the specified FTP/TFTP server via the FTP/TFTP protocol.

The configuration data hereby can be one or more than one type among user data, port data, protocol parameter data and default parameter data for guaranteeing the normal operation of the equipment. Of course, those skilled in the art should understand that the configuration data can also be other types of data besides the above mentioned ones.

In step 110, the procedure of backing up the configuration data is monitored. While backing up the configuration data, the IAD will report the current backup progress to the IADMS through the progress TRAP, so that the IADMS can acquire the backup status of the IAD through the progress TRAP received from the IAD, thus the monitor function is implemented.

In step 120, the IADMS judges whether the configuration data are successfully backed up, if yes, executing the next step 130; otherwise, returning to the step 100, which is to instruct the IAD to back up the configuration data over again, and the IAD will back up the configuration data over again after receiving this instruction.

The process of judging whether the configuration data are successfully backed up is to judge whether a backup failure TRAP is received or whether the backup procedure exceeds the scheduled time. If the IADMS receives the backup failure TRAP from the IAD or detects that the operating time of the backup procedure of the IAD exceeds the scheduled time, the IADMS confirms the backup has failed; otherwise, the backup is successful.

Moreover, after confirming the backup has failed, IADMS can notify a user that the current backup fails and that the user can choose whether to back up the data over again. After receiving the user's indication of backing up the data over again, the IADMS will instruct the IAD to back up the configuration data over again. If the user chooses not to back up the data anymore, the current process will be ended.

In step 130, the equipment software is updated. Firstly, the IADMS sends an SNMP update command to the IAD, and this command comprises updated FTP/TFTP server address, updated files name and other information. After receiving this command, the IAD analyzes it and downloads the updated files from the FTP/TFTP server via the FTP/TFTP protocol, according to the FTP/TFTP server address, the updated files name and other information comprised in this command. After downloading all the updated files, the IAD loads the updated files to implement the equipment software update.

In addition, as to some communication equipment, the loaded software is not effective until resetting the equipment. In this case, the IADMS needs to send an SNMP reset command to the IAD and request the IAD to reset. The IAD resets itself after receiving this SNMP reset command, so that the current loaded new software version can be effective. Of course, as to those communication equipment that can make the loaded software effective without resetting themselves, the above-illustrated reset process can be removed.

In step 140, the update procedure of the equipment software is monitored. While downloading and loading the updated files, the IAD will report the current update progress to the IADMS through the progress TRAP, so that IADMS can acquire the update status of the IAD through the progress TRAP received from the IAD, thus the monitor function is implemented.

In step 150, IADMS judges whether the equipment update is successful. If it is unsuccessful, it go to step 160, i.e., the IADMS will instruct the IAD to recover the old software version before the software update, and the IAD will automatically replace the current software with the old one after receiving this indication. If the IADMS judges that update is successful, it will execute the next step 170.

In the present embodiment, after the step 160, which means after the IAD has replaced the current software version with the old one, the step 130 will be automatically executed, which means the IADMS will instruct the equipment to execute the update process over again. As the update may be unsuccessful finally due to power off in the previous update procedure, executing the update process over again can guarantee the update function after the power is recovered; while if the update is unsuccessful because of

the updated files error, the IADMS can re-specify the correct updated files name in the SNMP update command sent to the IAD so as to make sure that the update is successful this time.

Of course, the IADMS can also notify the user of this situation after the IAD has recovered the old software version. The IADMS can also ask the user whether to update the equipment over again. After receiving the user's indication of updating equipment over again, the IADMS will instruct the IAD to execute the update operation over again. If the user chooses not to update anymore, the current process will be ended.

In the present invention, two memory buffers can be set inside the equipment to be updated, one for storing the software version before the update and the other for storing the new software version. In this way, if the current update is unsuccessful, the equipment can read the old software version from the memory buffer that stores the software version before update so as to recover the old software. Since the two software versions are stored in two memory buffers respectively, the unsuccessful update will not affect the software version before update, so that communication equipment can recover the complete old software and will not change into failure or fault because of the abnormal operation.

The procedure of judging whether the update is successful is to judge whether an update failure TRAP is received or whether the update operation exceeds the scheduled time. If the IADMS receives the update failure TRAP from the IAD or determines that the update operation of IAD exceeds the scheduled time, the update is deemed as unsuccessful, otherwise, the update is successful.

In step 170, the backup configuration data are recovered. The IADMS sends the recovery configuration data command to the IAD, and the command comprises the address information of the FTP/TFTP server which stores the configuration data, the configuration data files name and so on. After receiving this command, the IAD analyzes this command and downloads the configuration data from the corresponding FTP/TFTP server via the FTP/TFTP protocol according to the FTP/TFTP server address, the configuration data name and other information comprised in this command. After downloading all the configuration data files, the IAD loads the updated files.

In step 180, the recovery procedure of the configuration data is monitored. While

downloading the configuration data and loading the configuration data, the IAD will report the current progress to the IADMS through the progress TRAP, so that the IADMS can acquire the recovery status of the IAD through the progress TRAP received from the IAD, thus the monitor function is implemented.

In step 190, the IADMS judges whether the configuration data are successfully recovered, if yes, the equipment update procedure is successfully completed and the current process is ended. If the configuration data are not successfully recovered, the step 170 is executed, namely the IADMS instructs the IAD to recover the configuration data over again. After receiving this instruction, the IAD downloads and loads the configuration data over again.

The process of judging whether the configuration data are successfully recovered is to judge whether a recovery failure TRAP is received or whether the recovery procedure exceeds the scheduled time. If the IADMS receives the recovery failure TRAP from the IAD or determines that the recovery operation of the IAD exceeds the scheduled time, the IADMS confirms that the recovery operation fails; otherwise, the recovery operation is successful.

Moreover, after confirming that the recovery operation fails, the IADMS can notify the user that current recovery operation fails and asks the user whether to recover the data over again. After receiving the user's instruction of recovering the data over again, the IADMS instructs the IAD to recover the configuration data over again. If the user chooses not to recover the data anymore, the current process will be ended.

In some cases, like when the new software and old software are different from each other, it is needed to modify the configuration data properly, so that the configuration data can be successfully applied in the new software environment after being recovered, i.e. the configuration data can be successfully recovered. Hereby after the IAD resets in the above-mentioned step 170, the IADMS further judges whether it is needed to modify the configuration data, if yes, the IADMS notifies the user to modify the data or instructs the IAD to automatically modify the data by running an application program which is specially used for modifying the configuration data, and continues to execute the recovery operation for the configuration data in the step 170 after finishing the modification. Hereby,

the configuration data modification, like conversing configuration data's format, can make the new configuration data format accord with the requirement of the new software, so as to make sure the configuration data can be successfully applied in the new software environment.

In case of needing to modify the configuration data, the configuration data recovery may be unsuccessful finally because of the incorrect configuration data modification, when the IADMS finds the configuration data recovery unsuccessful, it will return to the process of instructing the user to modify the configuration data or instructing the IAD to run the application program to modify the configuration data. After the configuration data are correctly modified, the configuration data are recovered again so as to make sure the configuration data can be successfully recovered.

The above mentioned is just the preferred embodiment of the present invention and not used to confine the present invention. Any modification, equivalent substitute and improvement within the spirit of the present invention are with the protection scope of the present invention.